

# Data Quality Management Standard

<b>Standard owner:</b>	Chief Operating Officer
<b>Standard approver:</b>	BBB Executive Committee
<b>Approval date:</b>	2 <sup>nd</sup> May 2023
<b>Annual review date:</b>	April 2024
<b>Document owner:</b>	Managing Director, Data Management Office.

---

## 1. Purpose

### 1.1 Purpose

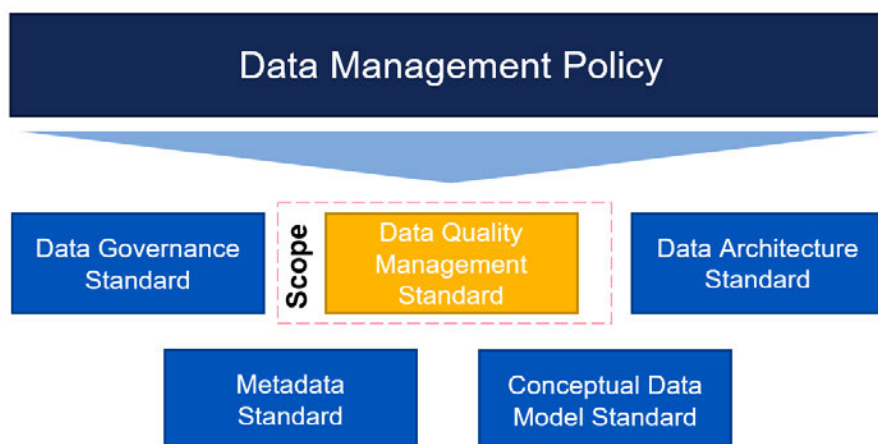
Data quality is commonly defined as accuracy, comprehensiveness, timeliness, and consistency of data. Data Quality Management is the establishment and implementation of data quality roles, responsibilities, standards, policies, procedures, and tools. When data is accurate, comprehensive, timely, and consistent with the end users' needs, it is referred to as 'fit for purpose'.

The adoption of this standard is mandatory to ensure that the implementation of the Data Management Policy in relation to Structured Data ("the Policy") is carried out appropriately and consistently across businesses functions at BBB.

This standard defines requirements for achieving 'fit for purpose' data, through establishment of a data quality strategy that encompasses managing, measuring, and governing the quality and consistency of BBB's data. The data quality strategy focusses on:

- **Establishing data quality controls, data profiling processes**
- **Development and implementation of data quality rules and issue management**
- **Performing data quality monitoring and reporting**
- **Understanding data quality tooling requirements**

This standard provides specific requirements to guide implementation of data quality controls, data profiling processes, implementation of data quality rules, reporting, issue management. This standard may require be applied to data acquired from a third party or vendor which is used as master or reference data.



---

## 2. Scope

This Policy and the associated Standards, apply to all BBB entities, operations, subsidiaries, and Colleagues (see Appendix A Policy Scoping, Policy Governance Framework for definitions) and interactions with Structured Data ("data"), from origination to processing, reporting and analytics.

Note: The Bank's Data Protection Policy and Information Security policies relate to issues of data protection and security, therefore are not covered in the Policy.

### 3. Key Requirements

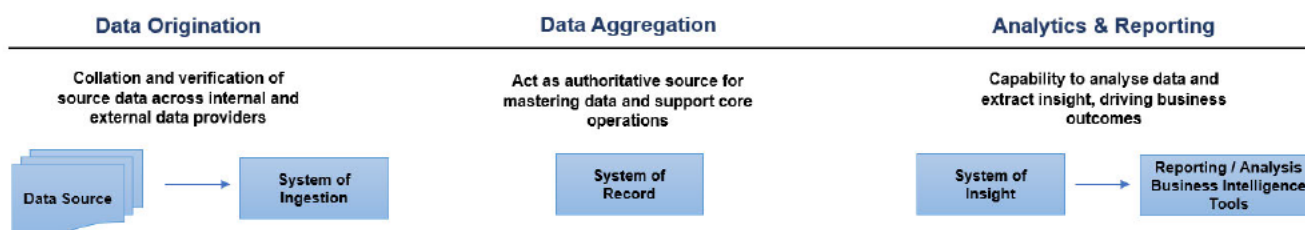
#### 3.1 Data Quality Management Strategy

The strategic direction for data quality at BBB emphasises that it must be managed at every stage in the data lifecycle of origination, aggregation, analytics and reporting. At each stage, data must be accurate, comprehensive, timely, and consistent. The strategy also emphasises that as the owner of data, it is the responsibility of the businesses and functions to prevent data quality exceptions and when identified, appropriately remediate them. Additionally, consumers of data are responsible for understanding the data they use for analytics and reporting, and to confirm they are 'fit for purpose'.

#### 3.2 Data Quality Management Processes

##### 3.2.1 Data Quality Profiling, Rules and Controls

The diagram below highlights how the data quality standards are leveraged across the data lifecycle:



At each stage of the data lifecycle, data must be assessed using the standard data quality dimensions:

Data Quality Dimensions	Objective
Accuracy	Ensures that the data being used for reporting matches with the known sources of truth (i.e. systems of ingestion, system of record or system of insight), which in turn correctly represent the entity, contract or other data concepts.
Completeness	Ensures that the rows of data (records) are the full set that is required for the usage.
Validity	Ensures that the data values conform to the data type, format and expected values for the element, and are valid.
Conformity	Ensures that relationships between individual data values, collectively conform to logical business rules which may involve a data concept.
Consistency	Ensures linkage between data across multiple sources is accurate and form a coherent data record.
Timeliness	Ensures that the data is as of the point in time and/or period required and is available within the elapsed time per requirements.
Uniqueness	Ensures that there is no duplication of source data at the record level that is expected to be unique.

## Data Quality Profiling

Data quality profiling focuses on examining data available within a data set and gathering statistics and information about that data. It helps not only to understand anomalies and to assess data quality, but also to discover, register, and assess metadata which is not previously available.

Data quality profiling is usually completed at the time of creation or modification of data (for example, following the system of ingestion), with results used to facilitate the creation and refinement of data quality rules and controls.

## Data Quality Rules

Data quality rules represent requirements defined by a central function or product team business, to enable the measurement and monitoring of data against the standard data quality dimensions of accuracy, completeness, validity, conformity, consistency, timeliness and uniqueness.

Implementation and development of rules is an iterative process. Application of the data quality rules is triggered by the origination of fresh data, to identify data quality exceptions at the earliest point in the data lifecycle.

## Data Quality Controls

### *Preventative Controls:*

Preventative controls may apply to data at any stage in the data lifecycle across any type of system or platform. These may include input controls, validation checks, and other preventative controls to ensure data meets business rules upon origination in systems of ingest, or aggregation within systems of record.

Where possible, the preventative controls would be applied at origination or as close as possible to help prevent data quality exceptions through following aggregation and analytics or reporting stages.

They are usually implemented by business functions, adopting built-in solutions and user interface design changes implemented through iterative product or software development activity.

Preventative controls must include validations controls and completeness controls.

- **Validation Controls:** Performed upon data capture typically where users interact through a user interface. Additional preventive data quality controls must check for the presence of defaulted values exceeding thresholds and capture of the correct data type.
- **Comprehensiveness Controls:** Performed upon data capture to measure the availability of all data as compared to the complete population of interest. Comprehensiveness controls, while primarily performed on the origination layer, may also be performed for aggregation and reporting layers, when appropriate to identify any potential data omissions.

### *Detective Controls:*

Detective controls typically apply to data at rest, including measuring against established business rules. They are designed to identify and discover data quality exceptions that may be introduced as data moves from origination to aggregation and reporting layers through the data lifecycle.

Detective controls require business functions to collaborate with end users and the Data Management Office (DMO) to institute effective management. These controls can be both automated (recommended) and manual (where necessary) and include cross system controls, as appropriate.

Such controls at the aggregation and reporting & analytical layers must:

- Cover the accuracy, completeness, validity, conformity, consistency, timeliness and uniqueness
- Evaluate quality of product information
- Check for conformance with specific risk requirements
- Assess transformations performed due to system/business drivers
- Enable cross system controls as data moves through the end-to-end system landscape

### 3.2.2 Data Quality Issue Management (DQIM)

Data quality issues are defined as defects that may have resulted in, but are not limited to, inaccurate, incomplete, untimely, and invalid data. These issues could be identified by data consumers, systems or tools that are designed to scan and detect large volumes of new source data or could be known issues that have existed for some time.

It is imperative that the Bank adopts a robust issue management framework with the ability to track the identification, analysis, and remediation of data quality issues through the issue management process. The DQIM tool will improve issue ownership and accountability, increase granularity, and provide transparency on issue remediation across all divisions and functions.

The scope of DQIM includes any data-driven processes that cause inaccurate reporting, process rework, missing or incomplete information, delayed processing, or any other negative process symptom that can create a data quality issue.

The scope of the DQIM includes any process involving data where data exceptions could negatively impact any business process or data quality dimensions.

#### Issue Identification

Scope	
Cause	Data quality issues should be captured regardless of the reason and the way the issue was identified. New issues, requirements and those that could lead to change requests to existing functionality should all be captured.
Occurrence	Data quality issues will typically be re-occurring and not one-off instances, however single occurrences of a problem may still qualify if they cause significant adverse impact to a business process and/or could occur again.
Dimension	Data quality issues should relate to data quality dimensions (e.g. timeliness, completeness or accuracy) and should be articulated from the point of view of the business which requires the data.
Production	Data quality issues should relate to production data only and not be related to any test data or testing environments.
Out of Scope	Architectural gaps, data access and the existence of data etc.



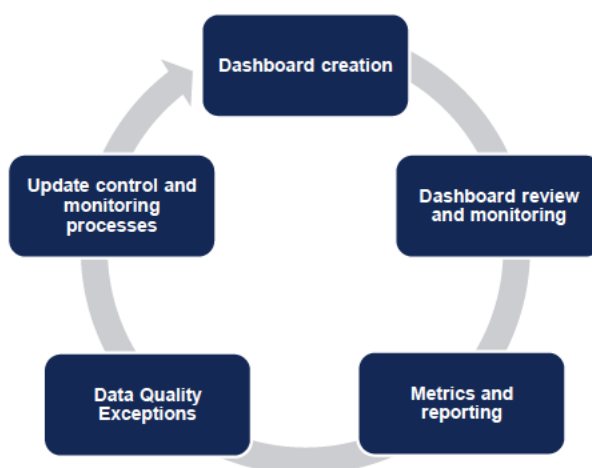
Granularity	
Specific	Related to an impacted business process and linked to a system of ingest, system of record, including identified data element(s).
	Data quality issues should be sized such that they can be owned by an identifiable Data Steward, subject matter expert, Data Custodian or Data Architect
	If there are both strategic and tactical fixes which need to be delivered, these can be identified within the same issue with differing remediation descriptions. Tactical and strategic solutions could have different priority, ownership, sponsors, analysts, benefits, timelines etc.
	Data quality issues which are raised and subsequently handed-off to another Product Team or Central Function for remediation cannot be consolidated with other issues (i.e. traceability needs to remain intact such that DMO retains visibility over the issue). However, issues may be linked if they are as a result of the same root cause.
Measurable	Sufficiently granular so that the benefit of remediation can be articulated. Additionally, if an issue requires 5 separate fixes before any benefit can be realised, this should remain as 1 issue in DQIM. However, if incremental benefit is realised after each fix, this can be captured in DQIM as 5 separate data issues.

### 3.2.3 Data Quality Monitoring and Reporting

Data quality monitoring and reporting is the continuous and proactive management of data to ensure data is 'fit for purpose'. The dashboards, metrics and reports are used to transparently provide insights into the state of data quality across the organisation. Additionally, the metrics provide transparency on key risks that impact data quality to Data Owners.

An effective monitoring & control reporting process is essential for continuous improvement, and ongoing monitoring, analysis, and planning drive additional assessment and improvement projects.

Outlined below are the core processes for ongoing data quality management:



#### Key Outcomes

- Dashboards present results from data quality assessments enabling Data Owners and Data Stewards to identify potential data quality exceptions or data integrity risks and record them using the DQIM process.

- Frequent reviews will highlight opportunities drive improvements in data quality.
- Highlight trends over time where slow and persistent changes in quality over time exist.
- Ensure prioritisation of data quality remediation and resource planning.
- Highlight repetitive exceptions and opportunities for preventative measures.

### 3.2.4 Data Quality Tooling

A centralised approach to running data quality checks must consider data quality tooling requirements to support the end-to-end process and detect data quality exceptions. The technology component provides a set of requirements covering tooling to support the governance, control and monitoring of data to ultimately ensure that data delivered to consumers to drive decision making is fit for purpose.

The following tooling requirements are structured to align with the Data Quality Management Methodology and provide context across the following:

- **Business Objectives** – outlines the business goals relevant for technology/tooling enablement.
- **Core Capabilities** – outlines the high-level technology/tooling enabled capabilities to enable business objectives to be met.

Tooling Requirement	Core Capabilities
DQ Profiling Tools	<ul style="list-style-type: none"> <li>➤ Provide a view of data structure, content, rules and relationships</li> <li>➤ Check key relationships are adhered to and referential integrity exists between columns and tables.</li> <li>➤ Test against data quality dimensions (i.e. completeness).</li> </ul>
Business Rules Management Tools	<ul style="list-style-type: none"> <li>➤ Business rules can be managed by DMO role holders directly rather than rely on the application of the rules by technical developers.</li> <li>➤ Rules can be re-usable and applied to multiple different data sets while being managed centrally.</li> </ul>
DQ Assessment Tools	<ul style="list-style-type: none"> <li>➤ Dashboard integration to support effective data quality monitoring and reporting.</li> </ul>

## 4. Roles and Responsibilities

All colleagues with responsibility for the origination, aggregation or analysis and reporting of data are responsible for the integrity of the data, including reports and documents, under their control. To ensure data quality is upheld throughout the data lifecycle, the following must be adhered to:

- All colleagues must be attentive to and vigilant about data quality.
- All colleagues that consume data must adhere to the principles and understand their intended purpose.
- All colleagues must communicate any data quality issues through the appropriate channels.
- All colleagues must source data from approved sources and avoid the creation of EUCs and individually owned datasets.
- All colleagues must understand and comply with the Data Quality Standard

## 4.1 Data Quality Analyst

### Role and Accountability/ Responsibility

The Data Quality Analyst sits within the DMO and will maintain data quality inventory, creating data quality control assessments and implementing any additional controls as required. Additionally, they will be responsible for performing regular data profiling and data quality assessments.

- **Accountable** for maintaining data quality rules and controls inventories.
- **Responsible** for using requirements provided by Data Domain Owner and Data Steward to create data profiling checks within the Data Quality toolsets. .
- **Responsible** for performing data profiling, data quality rules and control assessments on regular basis (i.e. monthly) and providing output to Data Steward for review.
- **Responsible** for supporting the Data Steward to capture data quality rules and control requirements, and additional refinements.
- **Responsible** for creating data quality rules and control assessments and implementing any additional rules and controls as required.
- **Responsible** for supporting Data Domain Owner to review data quality rules and controls.

## 4.2 Issue Raiser

### Role and Accountability/ Responsibility

The issue raiser can be any colleagues who will identify and log data quality issues within DQIM ensuring issue details are accurate and complete.

- **Responsible** for capturing the initial details of the issue, including issue summary, issue description and impacted business function and process.
- **Responsible** for identifying the Data Steward based on the impacted business function and process to support issue capture and populating remaining fields.

-

## 4.3 Data Domain Owner

### Role and Accountability/ Responsibility

The Data Domain Owner will oversee data quality issues and provide support with prioritisation and issue closure.

- **Responsible** for supporting the Data Steward for capturing requirements for definition of data profiling checks, additional data quality rules and controls associated with a specific data domain.
- **Accountable** for providing oversight and guidance on threshold allocation for each data quality rule.



- **Responsible** for performing periodic reviews of all data quality rules and, where applicable, challenging the data quality rules for efficiency and alignment with intended outcomes for business function processes.
- **Accountable** for providing oversight and guidance on threshold allocation for each data quality control.
- **Responsible** for conducting regular review of control effectiveness with Data Steward and Data Quality Analyst.

#### 4.4 Data Owner

##### Role and Accountability/ Responsibility

The Data Owner will chair relevant Business Function Forums and escalate any data related issues to the Data Governance Forum as required.

- **Responsible** for escalating data issues to the Data Governance Forum.

#### 4.5 Data Steward

##### Role and Accountability/ Responsibility

The Data Steward will proactively manage the issue, helping support across all remediation activities throughout the DQIM lifecycle. Work alongside Issue Raiser to review issue details and business impact before progressing to root cause analysis and identify solution design stages. They are responsible for providing issues requiring prioritisation and/or funding to Data Owner for escalation to relevant Data Governance Forum, and closing the issue once required sign-off has been obtained.

- **Responsible** for working with the Data Domain Owner on capturing requirements for definition of additional data quality rules and controls associated with a specific Data Domain.
- **Accountable** for reviewing data profiling results regularly and ad-hoc reviews when one or more trigger events are encountered:
  - o Trend analysis of data quality indicates a shift in the underlying data.
  - o Changes in business function processes resulting in a change in data architecture.
  - o A new data source is introduced.
- **Responsible** for working with Data Quality Analyst on capturing data quality rules based on 'fit for purpose' requirements pertinent for the business function process.
- **Responsible** for supporting the Data Domain Owner for reviewing data quality rules and control effectiveness.
- **Responsible** working with the Data Quality Analyst on capturing control requirements.
- **Responsible** for being the Action Owner for current action against issue captured by the DQIM (this will usually be you or the Data Custodian, determined by the issue status).

## 4.6 Data Custodian

### Role and Accountability/ Responsibility

Data Custodians are usually IT points of contact or IT product owners that are responsible for ensuring that systems and platforms deliver effective business processes and functionality, and accurate and controlled origination, integration, access control, and storage of data at the application level.

The Data Custodian, in collaboration with Data Stewards will support data quality issue root cause analysis and issue remediation through effective change management, particularly including the implementation of preventative data quality controls.

- **Responsible** for Implementing data quality rules and controls. .
- **Responsible** for proposing the final solution design for the data issue and involved in implementing the execution and delivery of the solution.

## 5. Further Reading

Further reading: Data Management Policy, Data Governance Standard

## 6. Policy Controls

Controls in place regarding this policy are as follows:

Control Reference	Control Title	Description	Frequency
DM-001	Data Governance Roles	All business areas must assign a Data Owner and Data Steward. All systems must have an assigned Data Custodian. Each data domain must have an assigned Data Domain Owner.	Continuous
DM-002	Critical Data Elements (CDE) Identified and Under Governance	<p>Critical Data Elements (CDEs) are data elements used for making business decisions that have an impact on the bank's financial performance, results, or bottom line.</p> <p>This control requires that CDEs must be defined and grouped within the business objects hierarchy with associated metadata, data sources, lineage and governance roles recorded and maintained.</p>	Continuous
DM-003	Preventative Data Quality	Preventative data quality controls (e.g. input validations) must be implemented for critical data elements.	Continuous
DM-004	Detective Data Quality	Detective data quality controls (data quality measurement) must be implemented for critical data elements.	Monthly
DM-005	Issue Management	A data quality issue management process is in place.	Monthly
DM-006	Systems of record	<p>System of Record is where the data is screened, managed, updated, deleted or mastered, validated and where exceptions are remediated.</p> <p>This control requires that each CDE has a designated system of record (which cannot be an end-user repository) with appropriate controls,</p>	Continuous




		where the data is managed, updated, deleted or mastered, validated and where exceptions are remediated.	
<b>DM-007</b>	Data Assessment as part of Change Initiatives	Data Assessments must be performed as part of the evaluation and design of changes and solutions to ensure data architecture principles are followed.	<b>Continuous</b>

## 7.

### Definition of Terms

Term	Definition
<b>BBB or the bank</b>	The British Business Bank plc ("BBB" or "the bank") and its subsidiaries.
<b>Colleagues</b>	Permanent Employees, Fixed Term Contract, Apprentices, Interns, Seconded-out, Seconded-In, Board Members, Non-Executive Directors, Contractors, Temps and Professional Services.
<b>End User Computing (EUC)</b>	EUC solutions refer to a range of tools adopted by individual data users to acquire, process and conduct analysis on data. Typically, in the format of excel files, access databases or Power BI reports (not limited to the list). An EUC is regarded as a sub-type of application.

### Version control

Version	Date	Author	Description	Approved by	Date approved	Date published
	11/06/2021		First draft			
	15/09/2021		Updated Section 7. Definition of terms to be consistent with 'the Policy'			
	22/10/2021		Version 1.0 Final Approved by BBB Board on 22 October 2021	BBB Board	22/10/2021	11/11/2021
	22/02/2023		Version 2.0 DRAFT for PRG Annual Policy Review			

Appendix 1 - Policy Scope Categories

Accurate policy scoping is important to ensure that those who might be affected by a policy are identified and considered.

The proposed approach is to capture all potential individuals and entities that could fall within scope of a BBB policy into 3 distinct categories:

- Personnel
- Colleagues
- Employees

Policy owners will be responsible for identifying which category is applicable to their policy.

Personnel													
Colleagues													
Employees													
Permanent Employees (Full or Part time)	Fixed term contract employees (FTC)	Apprentices	Interns	Secondees - out	Secondees - in	Board Members (executive directors)	Non-executive directors (NEDs)	Contractors	Temps	Professional Services	Agents	Representatives	Third Parties

The Policy Governance Framework will capture the detailed list of which individuals fall within each category for reference. (Slide 3).

Policy Scope wording:

This policy applies to all BBB entities, operations and Personnel.

This policy applies to all BBB entities, operations and Colleagues.

This policy applies to all BBB entities, operations and Employees.